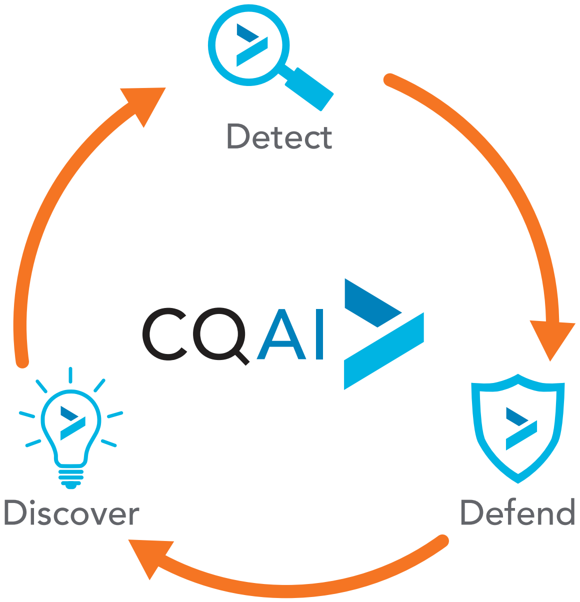
CEQUENCE™ SECURITY

CQAI Engine

AI-Powered Intelligence for Stronger Application Security

The CQAI Engine is at the core of the Cequence ASP Platform, providing the intelligence to automatically discover all applications, detect threats, and provide policy-based defense.

The CQAI analyzes traffic to proactively reveal all applications including web, mobile, or API-based apps. Next, CQAI uses multidimensional AI-powered analytics to detect malicious bot behaviors down to the level of intent. This passive analysis requires no modification to your apps and has no impact on performance. Once threats are found, CQAI works with all CQ security service modules to provide a range of automated protections to mitigate threats and deceive attackers actively.



Discover and Cover All Your Apps

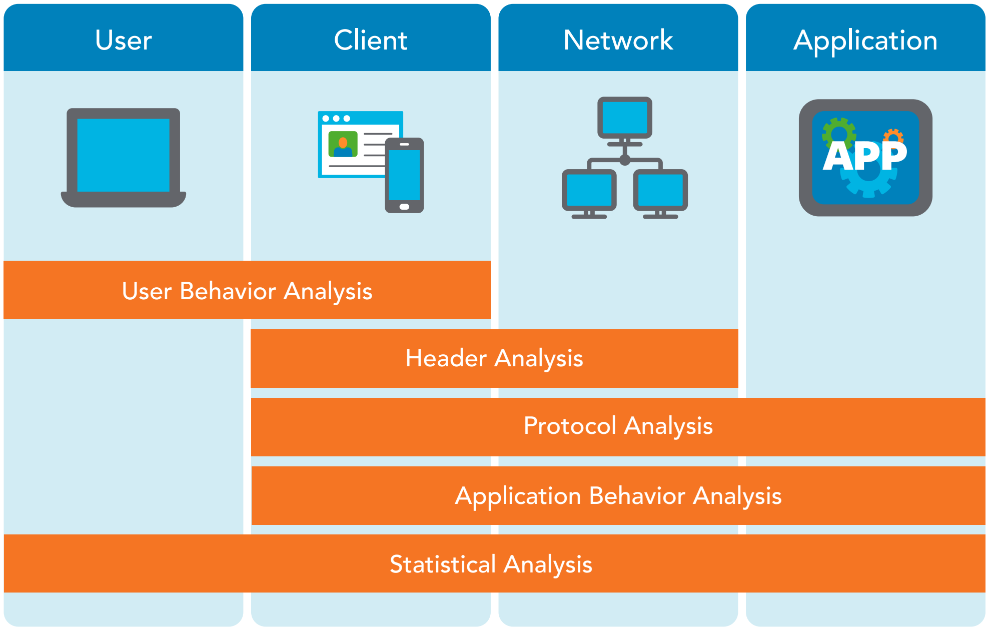
Traditional bot and web defenses require security teams to pick and choose where to defend by requiring customization of each app and interface - often for additional costs. Cequence's distributed, network-based architecture lets organizations secure all of their applications from a single deployment including all web, mobile, and API-based apps - without any modification required. Just as importantly, CQAI's built-in intelligence automatically identifies all applications across the organization, even if they are unknown to security teams. As developers roll out new applications and updates, Cequence security adapts automatically. With the combination of architecture and CQAI intelligence, Cequence ASP provides the only solution to cover your entire application attack surface reliably.

Multidimensional AI-Based Threat Detection

CQAI's unique blend of AI and machine learning enables threat detection that accurately identifies more attacks, is more reliable, and has no impact on performance. CQAI begins by analyzing every interaction from multiple perspectives including client, network, and application traits and behaviors. This gives the engine a much more complete view of behavior than what is possible with technologies that rely on client context alone. For example, while client-side analysis can reveal unusual header anomalies, an application-side analysis can see the actual attack behavior of a denial of inventory attack where a user repeatedly puts items in his basket without purchasing. Blending these perspectives makes CQAI much more insightful and reliable.

The engine then uses an ensemble of AI, machine learning models, behavioral analysis, and statistical analysis of hundreds of traits to identify threats. This includes, but is not limited to, heuristic analysis of headers, protocols, other network traffic, and both user and application behavior. The system also performs a statistical analysis of all of these traits to identify patterns and anomalies. By tracking the unique multi-step behaviors of real attacks, the CQAI engine can even distinguish malicious bots from benign forms of automation such as approved content aggregators.

When a threat is detected, CQAI builds a fingerprint of the attacker based on the attack tools used, the infrastructure and behavior. And while it is easy for attackers to move to new IP addresses constantly, their fundamental tools and behavior remain the same, allowing staff to track and respond to attackers instantly. By blending multiple perspectives and types of analysis, CQAI provides an accurate, low-impact approach that detects threats others miss while reducing false positives.



CQAI works in concert with Cequence security modules. The first security module is CQ botDefense which focuses on detection and prevention of malicious bots. As new security modules are released, the power of CQAI is easily extended to address additional threats and use cases.

Threat-Appropriate Mitigation

Even though detection is purely passive, Cequence's unique architecture enables instant mitigation once a threat is detected. Responses are automated by policy, and IT staff can choose from a variety of mitigation options based on the threat, including blocking of content scrapers, rate limiting DoS behaviors, or active deception of new account creation attacks. Integration with CQ Connect can also be used to integrate with other systems and automatically trigger actions such as blocking at a WAF or firewall.

Deception offers a particularly powerful counter to automated attacks. For instance, deception can make an attacker believe a credential stuffing attack was successful. This disrupts the attack, feeds the attacker back bad data, and allows security to observe the attackers next steps and long-term intent, all while preventing the attacker from consuming resources of the actual application.

Extensible and Open

The CQAI makes use of Cequence security service modules such as CQ botDefense. Each module provides content and intelligence tied to a specific use case or style of threat. This modular design allows teams to expand their use the Cequence ASP platform over time, and to perform multiple security functions that leverage a single-pass architecture.

CQAI is also an open system that shares granular details on detections and even allows users to write their own detection logic. While many AI and ML-based systems function like isolated "black boxes," CQAI can share underlying detection metadata through CQ Connect. This lets security analysis and data scientists correlate CQAI data with their other systems and data sources. Likewise, if data scientists or developers identify new detection patterns based on their analysis, they can easily write detection models to run within CQAI.

You can also learn more about the Cequence Application Security Platform by visiting our website's resources section: cequence.ai/resources.

CEQUENCE™ SECURITY

100 Murphy Avenue, Suite 300, Sunnyvale, CA 94086 › 1-408-978-3258 › info@cequence.ai › www.cequence.ai